ZUSATZVEREINBARUNG

Datensouveränität und Ausschluss von Zugriffen ausländischer Behörden

(insbesondere im Anwendungsbereich des U.S. CLOUD Act)

als Anlage zur Vergabe Nr. _____
für Managed Extended Detect and Response (MXDR) Dienstleistungen zwischen

Stadt Mölln, Wasserkrüger Weg 16, 23879 Mölln – nachfolgend „Auftraggeber" –

und

_____

– nachfolgend „Auftragnehmer" –

– gemeinsam „Parteien" –

> ***Hinweis:*** *Diese Anlage ersetzt keinen Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DSGVO, sondern ergänzt ihn um spezifische Regelungen zur Datensouveränität. Den AVV legt der Auftragnehmer nach Maßgabe der Anlage 3 zum Leistungsverzeichnis zur Abstimmung und Unterschrift vor; im Kollisionsfall regelt Ziffer 12 den Vorrang.*

1. Präambel

Der Auftraggeber beschafft einen Managed-Detection-and-Response-Dienst (MXDR) für seine Clients und Server. Dabei verarbeitet der Auftragnehmer Telemetrie- und Protokolldaten aus der IT-Infrastruktur des Auftraggebers sowie im Einzelfall Inhalte von Endgeräten, darunter personenbezogene Daten von Beschäftigten sowie von Bürgerinnen und Bürgern. Die Parteien sind sich einig, dass ein Zugriff ausländischer Behörden oder Gerichte auf diese Daten außerhalb geltender Rechtshilfeabkommen mit der Europäischen Union bzw. der Bundesrepublik Deutschland zu vermeiden ist. Dies betrifft insbesondere, aber nicht ausschließlich, Anordnungen auf Grundlage des U.S. Clarifying Lawful Overseas Use of Data Act („CLOUD Act", 18 U.S.C. § 2713) sowie vergleichbarer Rechtsakte anderer Drittstaaten. Den Parteien ist bewusst, dass ein Unternehmen, das der Rechtsordnung eines Drittstaats unterliegt, eine Herausgabe nicht in jedem Fall rechtlich verweigern kann. Diese Vereinbarung verbindet deshalb vertragliche Zusicherungen mit technischen und organisatorischen Maßnahmen, die einen solchen Zugriff verhindern oder wesentlich erschweren.

2. Begriffsbestimmungen

- „Drittstaat" bezeichnet jeden Staat außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums (EWR), unabhängig davon, ob für ihn ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO besteht; dies gilt insbesondere auch für die Vereinigten Staaten von Amerika.
- „Behördliche Anordnung" bezeichnet jedes Auskunfts-, Herausgabe-, Zugriffs- oder Offenlegungsverlangen einer Behörde, eines Gerichts oder einer sonstigen staatlichen Stelle eines Drittstaats, unabhängig davon, ob es sich um eine Anordnung, einen Beschluss, eine Vorladung („subpoena"), einen „National Security Letter" oder eine vergleichbare Maßnahme handelt.
- „Rechtshilfeabkommen" bezeichnet ein völkerrechtliches Abkommen über Rechtshilfe in Straf- oder Zivilsachen (z. B. Mutual Legal Assistance Treaty, MLAT) zwischen der Bundesrepublik Deutschland bzw. der Europäischen Union und dem jeweiligen Drittstaat, das ein Ersuchen über die zuständigen Behörden der Bundesrepublik Deutschland bzw. eines Mitgliedstaats vorsieht. Ein künftiges Abkommen zwischen der Europäischen Union und den Vereinigten Staaten über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln gilt als Rechtshilfeabkommen, sobald und soweit es in Kraft ist.

- „Vertragsdaten“ bezeichnet sämtliche im Rahmen der Vertragsdurchführung durch den Auftragnehmer oder seine Unterauftragsverarbeiter verarbeiteten, gespeicherten oder übermittelten Daten des Auftraggebers, einschließlich personenbezogener Daten im Sinne des Art. 4 Nr. 1 DSGVO, Telemetrie- und Protokolldaten, Metadaten, Datei-Samples, Erkennungs- und Vorfalldaten, Konfigurationsdaten sowie daraus abgeleiteter Informationen, unabhängig davon, ob sie vom Auftraggeber bereitgestellt oder von der eingesetzten Software beim Auftraggeber erzeugt werden. Ausgenommen sind anonymisierte Erkennungsmerkmale ohne Personenbezug und ohne Bezug zum Auftraggeber (z. B. Hashwerte von Schadsoftware, IOCs).
- „Inhaltsdaten“ bezeichnet Inhalte von Dateien, Dokumenten, E-Mails und sonstigen Nachrichten auf Endgeräten des Auftraggebers, nicht jedoch Metadaten und Telemetrie.
- „Zugriff“ bezeichnet jede Kenntnisnahme, Einsichtnahme oder Übermittlung von Vertragsdaten, einschließlich eines Fernzugriffs von einem Ort außerhalb der EU/des EWR.

3. Ort der Datenverarbeitung

Der Auftragnehmer stellt sicher, dass die Vertragsdaten ausschließlich in Rechenzentren innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums gespeichert und verarbeitet werden. Eine Verarbeitung, Spiegelung, Sicherung (Backup), ein Zugriff oder eine sonstige Übermittlung von Vertragsdaten außerhalb der EU/des EWR ist unzulässig, es sei denn, der Auftraggeber hat dem im Einzelfall vorher in Textform zugestimmt.

Der Auftragnehmer legt dem Auftraggeber auf Verlangen den konkreten Verarbeitungsort (Standort des Rechenzentrums) sowie sämtliche Standorte, an denen Vertragsdaten repliziert, gesichert oder zwischengespeichert werden, offen.

4. Kein Zugriff durch Drittstaaten-Behörden

Der Auftragnehmer sichert zu, dass weder er selbst noch von ihm eingesetzte Unterauftragsverarbeiter behördlichen Anordnungen von Drittstaaten Folge leisten, die auf Herausgabe, Offenlegung oder Zugriff auf Vertragsdaten gerichtet sind, sofern nicht ein Rechtshilfeabkommen die Grundlage bildet und die zuständige Behörde der Bundesrepublik Deutschland bzw. des betroffenen Mitgliedstaats die Übermittlung nach Maßgabe dieses Abkommens bewilligt hat.

Dies gilt unabhängig davon, ob der Auftragnehmer selbst, ein mit ihm verbundenes Unternehmen (§ 15 AktG) oder ein Unterauftragsverarbeiter der Anordnung eines Drittstaats unterliegt, insbesondere im Fall von Konzernkonstellationen mit Sitz, Mutter- oder Tochtergesellschaften in einem Drittstaat, aus denen ein extraterritorialer Zugriffsanspruch abgeleitet werden könnte (z. B. gemäß CLOUD Act).

Kann der Auftragnehmer die Zusicherung nach Absatz 1 aus rechtlichen Gründen nicht oder nicht vollständig abgeben, insbesondere weil er, ein verbundenes Unternehmen oder ein Unterauftragsverarbeiter der Rechtsordnung eines Drittstaats unterliegt, gilt Ziffer 4a. Dies ist kein Ausschlussgrund im Vergabeverfahren.

Der Auftragnehmer teilt dem Auftraggeber unverzüglich in Textform mit, wenn sich die Beherrschungsverhältnisse bei ihm oder beim Hersteller der eingesetzten Plattform so ändern, dass ein Unternehmen mit Sitz in einem Drittstaat beherrschenden Einfluss erlangt.

4a. Ersatzmaßnahmen bei fehlender Zusicherung

In den Fällen der Ziffer 4 Absatz 3 legt der Bieter mit dem Angebot dar,

- welche Gesellschaften welcher Drittstaaten einen Zugriff auf Vertragsdaten anordnen lassen könnten und auf welcher Rechtsgrundlage,
- welche technischen und organisatorischen Maßnahmen einen Zugriff auf Vertragsdaten im Klartext verhindern oder wesentlich erschweren, insbesondere Schlüsselhoheit des Auftraggebers oder eines Treuhänders in der EU, Betrieb und Administration ausschließlich durch Personal in der EU/im EWR ohne Weisungsbindung an die Drittstaaten-Gesellschaft sowie technische Trennung der Datenhaltung, und
- welche Vertragsdaten trotz dieser Maßnahmen einem Zugriff ausgesetzt bleiben.

Die dargelegten Maßnahmen werden Vertragsbestandteil. Die Ziffern 5, 6, 8 und 9 bleiben unberührt. Ein Verstoß gegen die nach dieser Ziffer vereinbarten Maßnahmen steht einem Verstoß gegen Ziffer 4 gleich.

5. Melde- und Informationspflichten bei behördlichen Anfragen

Erhalten der Auftragnehmer oder ein Unterauftragsverarbeiter Kenntnis von einer behördlichen Anordnung, einem Ersuchen oder einer sonstigen Aufforderung eines Drittstaats, die sich auf Vertragsdaten bezieht oder beziehen könnte, informiert der Auftragnehmer den Auftraggeber unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, in Textform. Die Information umfasst mindestens:

- die anfragende Stelle und die Rechtsgrundlage der Anordnung,
- den Umfang der verlangten Daten,
- die gesetzte Frist zur Beantwortung bzw. Herausgabe,
- die vom Auftragnehmer beabsichtigten oder bereits ergriffenen Maßnahmen.

Ist dem Auftragnehmer die Benachrichtigung des Auftraggebers durch ein gesetzliches Verbot („gag order“) untersagt, informiert er den Auftraggeber, sobald und soweit dies rechtlich zulässig ist, und dokumentiert die Gründe der Verzögerung. Er bemüht sich mit allen zumutbaren rechtlichen Mitteln um die Aufhebung des Verbots. Für die Dauer des Verbots liegt kein Verstoß gegen die Frist nach Absatz 1 vor.

6. Widerspruchs- und Rechtsmittelpflicht

Der Auftragnehmer verpflichtet sich, jede behördliche Anordnung eines Drittstaats, die sich auf Vertragsdaten bezieht und nicht auf einem Rechtshilfeabkommen beruht, mit allen ihm zumutbaren rechtlichen Mitteln anzufechten bzw. ihr zu widersprechen. Dies umfasst insbesondere die Prüfung und Geltendmachung von Zuständigkeits- und Verhältnismäßigkeitseinwänden, die Berufung auf entgegenstehendes Recht der Europäischen Union und ihrer Mitgliedstaaten, das Verlangen, die anordnende Stelle an den Auftraggeber zu verweisen, sowie die Einlegung von Rechtsmitteln, soweit diese nach Einschätzung eines qualifizierten Rechtsberaters hinreichende Aussicht auf Erfolg haben. Der Auftragnehmer legt die Anordnung so eng wie möglich aus und gibt nur die Daten heraus, zu deren Herausgabe er nach abschließender Entscheidung verpflichtet ist.

Der Auftraggeber ist berechtigt, sich einem solchen Verfahren auf eigene Kosten anzuschließen oder den Auftragnehmer bei der Rechtsverteidigung zu unterstützen; der Auftragnehmer wirkt hieran nach Kräften mit.

7. Technische und organisatorische Maßnahmen

Zur Absicherung der in Ziffer 3 bis 6 geregelten Pflichten setzt der Auftragnehmer mindestens folgende technische und organisatorische Maßnahmen um:

- Verschlüsselung der Vertragsdaten nach dem Stand der Technik (Orientierung: BSI TR-02102), sowohl bei der Übertragung („in transit“) als auch bei der Speicherung („at rest“);
- Protokollierung sämtlicher Zugriffe auf Vertragsdaten, insbesondere administrativer Zugriffe und Fernzugriffe auf Endpunkte, mit manipulationsgeschützter Aufbewahrung der Protokolle für mindestens 12 Monate und Einsicht für den Auftraggeber auf Verlangen;
- Zugriffe auf Vertragsdaten nur durch Personal, das sich in der EU/im EWR aufhält, soweit der Auftraggeber nicht im Einzelfall vorher in Textform einem Zugriff aus einem Drittstaat zugestimmt hat (z. B. für Hersteller-Support bei einem Vorfall);
- Umsetzung der angebotenen Schlüsselverwaltung durch den Auftraggeber oder einen Treuhänder (Bring/Hold Your Own Key), soweit angeboten; der Auftraggeber kann den Schlüssel jederzeit sperren (Einzelheiten nach Wertungskriterium [B6] der Bewertungsmatrix);
- Übermittlung von Datei-Samples nur an Analysedienste innerhalb der EU/des EWR; Funktionen, die Vertragsdaten an Stellen außerhalb der EU/des EWR übermitteln, sind deaktiviert;
- keine Nutzung von Vertragsdaten für eigene Zwecke des Auftragnehmers oder des Herstellers, insbesondere nicht zum Training von KI-Modellen.

8. Unterauftragsverarbeiter

Der Auftragnehmer legt dem Auftraggeber vor Vertragsschluss sämtliche eingesetzten Unterauftragsverarbeiter sowie deren Sitz, Konzernzugehörigkeit und Verarbeitungsort offen. Der Austausch oder die Hinzuziehung weiterer Unterauftragsverarbeiter ist mindestens 30 Tage im Voraus anzukündigen und bedarf der vorherigen Zustimmung des Auftraggebers in Textform; dieser kann die Zustimmung verweigern, wenn der neue Unterauftragsverarbeiter die Anforderungen dieser Vereinbarung nicht erfüllt.

Der Auftragnehmer stellt sicher, dass sämtliche Verpflichtungen dieser Anlage im Wege inhaltlich gleichwertiger vertraglicher Verpflichtungen („flow-down“) an alle Unterauftragsverarbeiter weitergegeben werden. Soweit ein Unterauftragsverarbeiter (z. B. ein Anbieter von Cloud-Infrastruktur) nur seine Standardbedingungen akzeptiert, legt der Auftragnehmer dar, inwieweit diese den Anforderungen dieser Vereinbarung entsprechen; Ziffer 4a gilt entsprechend.

9. Nachweis- und Prüfrechte

Der Auftragnehmer weist die Einhaltung dieser Vereinbarung durch geeignete Nachweise nach, insbesondere durch:

- ein aktuelles Testat nach BSI C5 (Typ 1 oder Typ 2) oder einen gleichwertigen Nachweis gemäß Leistungsverzeichnis, auf Verlangen des Auftraggebers;
- einen jährlichen Transparenzbericht, jeweils bis zum 31. März für das vorangegangene Kalenderjahr, mit Angaben zu Anzahl, anfragender Stelle, Rechtsgrundlage und Umgang mit behördlichen Anordnungen von Drittstaaten im Sinne von Ziffer 5; soweit das anwendbare Recht nur zusammengefasste Angaben (z. B. Spannbreiten) erlaubt, genügen diese;
- die Ermöglichung von Audits durch den Auftraggeber oder einen von ihm beauftragten unabhängigen Dritten mit einer Ankündigungsfrist von in der Regel 14 Tagen, bei konkreten Anhaltspunkten für einen Verstoß auch kurzfristiger.

10. Vertragsstrafe

Verstößt der Auftragnehmer schuldhaft gegen die in dieser Vereinbarung geregelten Pflichten, verwirkt er eine Vertragsstrafe; ein Verschulden seiner Unterauftragsverarbeiter wird ihm zugerechnet. Die Höhe der Vertragsstrafe richtet sich nach der Schwere des jeweiligen Verstoßes gemäß nachstehender Staffelung:

Schweregrad	Erfasste Pflichtverletzung	Vertragsstrafe je Verstoß
Leicht	Verstoß gegen die Melde- und Informationspflichten nach Ziffer 5 (z. B. Überschreitung der 24-Stunden-Frist), ausgenommen die Dauer eines gesetzlichen Mitteilungsverbots; Überschreitung der vom Auftragnehmer nach Wertungskriterium [B7] der Bewertungsmatrix zugesagten Meldefrist für Sicherheitsvorfälle	0,5 % der Jahresvertragssumme
Mittel	Verstoß gegen die Widerspruchspflicht (Ziffer 6), die technischen und organisatorischen Maßnahmen (Ziffer 7), die Pflichten zu Unterauftragsverarbeitern (Ziffer 8) oder die Nachweispflichten (Ziffer 9)	2 % der Jahresvertragssumme
Schwer	Verstoß gegen Ziffer 3 (Verarbeitungsort außerhalb EU/EWR), Ziffer 4 (tatsächliche Befolgung einer behördlichen Anordnung eines Drittstaats ohne Rechtshilfeabkommen) oder die nach Ziffer 4a vereinbarten Maßnahmen	5 % der Jahresvertragssumme

Die Summe aller innerhalb eines Vertragsjahres verwirkten Vertragsstrafen ist auf 10 % der Jahresvertragssumme begrenzt (Gesamtobergrenze). Mehrere Verstöße gegen dieselbe Pflicht innerhalb desselben Lebenssachverhalts gelten als ein Verstoß.

„Jahresvertragssumme“ im Sinne dieser Ziffer ist die Nettovergütung, die dem Auftragnehmer aus dem Hauptvertrag für die zwölf Monate vor dem jeweiligen Verstoß zusteht; ist der Vertrag zu diesem Zeitpunkt noch keine zwölf Monate in Kraft, ist die Nettovergütung für das erste Vertragsjahr nach dem Angebot (Pos. 1.1 und 1.2 des Leistungsverzeichnisses) maßgeblich.

Die Geltendmachung eines darüberhinausgehenden Schadens bleibt unberührt; die gezahlte Vertragsstrafe wird auf einen etwaigen Schadensersatzanspruch angerechnet. Der Auftraggeber kann die Vertragsstrafe bis zur Schlusszahlung geltend machen, auch wenn er sie sich bei Annahme der Leistung nicht vorbehalten hat.

Klarstellung zum Verhältnis der Service Level-Gutschriften zur Vertragsstrafe

Die in Anlage 1 zum Leistungsverzeichnis (Service Level) vorgesehenen Gutschriften bei Nichteinhaltung der vereinbarten Service Levels sind eigenständige vergütungsbezogene Rechtsfolgen und werden auf die in Nr. 10 dieser Zusatzvereinbarung geregelte Vertragsstrafe nicht angerechnet.

Die Begrenzung der Vertragsstrafe auf insgesamt 10 % der Jahresvertragssumme bezieht sich ausschließlich auf die Vertragsstrafe gemäß Nr. 10 dieser Zusatzvereinbarung. Die Begrenzung der SLA-Gutschriften auf 15 % der jeweiligen monatlichen Vergütung bleibt hiervon unberührt.

Soweit die Voraussetzungen der jeweiligen Regelungen erfüllt sind, können SLA-Gutschriften und Vertragsstrafe nebeneinander geltend gemacht werden. Eine doppelte Kompensation desselben Schadens über darüber hinausgehende Schadensersatzansprüche bleibt ausgeschlossen.

11. Außerordentliches Kündigungsrecht

Der Auftraggeber ist zur außerordentlichen Kündigung des Hauptvertrags aus wichtigem Grund berechtigt, wenn

- der Auftragnehmer einer behördlichen Anordnung eines Drittstaats entgegen Ziffer 4 nachkommt, ohne dass ein Rechtshilfeabkommen dies deckt, oder die nach Ziffer 4a vereinbarten Maßnahmen nicht nur unerheblich verletzt,

- der Auftragnehmer wiederholt oder schwerwiegend gegen die Melde-, Widerspruchs- oder Nachweispflichten dieser Vereinbarung verstößt,
- sich herausstellt, dass die Voraussetzungen der Ziffer 3 (Verarbeitungsort EU/EWR) tatsächlich nicht eingehalten wurden, oder
- ein Unternehmen mit Sitz in einem Drittstaat beherrschenden Einfluss auf den Auftragnehmer oder den Hersteller der eingesetzten Plattform erlangt und der Auftragnehmer nicht innerhalb von drei Monaten gleichwertige Maßnahmen nach Ziffer 4a nachweist.

Im Kündigungsfall unterstützt der Auftragnehmer den Auftraggeber bei der Migration der Vertragsdaten zu einem Nachfolgeanbieter. Es gelten die Regelungen zum Exit-Management im Leistungsverzeichnis; die Übergabe der Daten erfolgt spätestens vier Wochen nach Zugang der Kündigung. Der Auftragnehmer löscht die Vertragsdaten nach Bestätigung des vollständigen Datenempfangs durch den Auftraggeber und bestätigt die Löschung in Textform.

12. Verhältnis zu anderen Vertragsdokumenten

Diese Anlage konkretisiert und ergänzt den Hauptvertrag Ausschreibung Nr. [einfügen] sowie den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Bei Widersprüchen gilt folgende Rangfolge: (1) diese Zusatzvereinbarung, (2) das Leistungsverzeichnis mit seinen Anlagen, (3) der Auftragsverarbeitungsvertrag, (4) der Hauptvertrag einschließlich seiner Vertragsbedingungen, (5) das Angebot des Auftragnehmers. Allgemeine Geschäftsbedingungen des Auftragnehmers finden keine Anwendung.

13. Schlussbestimmungen

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz des Auftraggebers.

Unterschriften

Ort, Datum: _____ Ort, Datum: _____

Für den Auftraggeber Für den Auftragnehmer